IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 4, July-August 2025

Impact Factor: 8.152

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

Security-Enhanced Blockchain Architecture

Vignesh K S, Vasantha, Vaishnavi, R Dhivya

Department of MCA, CMR Institute of Technology, Bengaluru, India

Department of MCA, CMR Institute of Technology, Bengaluru, India

Department of MCA, CMR Institute of Technology, Bengaluru, India

Assistant Professor, CMR Institute of Technology, Bengaluru, India

ABSTRACT: This paper presents a security-enhanced blockchain architecture designed to mitigate critical vulnerabilities found in both traditional digital systems and existing blockchain frameworks. The proposed model introduces a multi-layered design that integrates advanced cryptographic safeguards, consensus-driven validation mechanisms, and automated smart contract functionalities to create a resilient, tamper-proof, and efficient system. The core innovations include the integration of a decentralized Public Key Infrastructure (PKI) to eliminate single points of failure, a Real-Time Anomaly Detection Engine for proactive threat mitigation, and a modular design that ensures network scalability and interoperability. The effectiveness and practical relevance of this architecture are confirmed by conceptual implementations in two high-impact sectors: healthcare record management and cryptocurrency transaction ledgers. These use cases demonstrate the system's capability to securely manage sensitive data while enabling trustless, automated transactions within a distributed environment.

KEYWORDS: Consensus mechanisms, Cryptographic data protection, Fault-tolerant distributed systems, Immutable transaction records, Network scalability optimization, Smart contract enforcement.

I. INTRODUCTION

Blockchain technology is reshaping industries by delivering secure, transparent, and decentralized solutions. It is increasingly recognized as a cornerstone of next-generation digital infrastructure, enabling the creation of systems which are not just secure but also intelligent. An important advantage of blockchain is its capacity to enhance cybersecurity: every transaction is recorded permanently within a data block and cryptographically connected to the preceding one through a unique hash. This design preserves data integrity, ensures tamper resistance, and minimizes the likelihood offraud.

Despite its potential, blockchain still faces several unresolved challenges. Scalability limitations restrict transaction throughput, while network latency hinders real-time responsiveness. In addition, the technology remains vulnerable to advanced threats such as Distributed Denial-of-Service (DDoS), Sybil, and Man-in-the-Middle (MITM) attacks. Issues of cross-chain interoperability and regulatory uncertainty further complicate widespread adoption.

In response to these issues, this paper proposes a multi-layered framework designed to strengthen blockchain's resilience and adaptability. The framework integrates decentralized Public Key Infrastructure (PKI), a Real-Time Anomaly Detection Engine, and a modular system architecture. Together, these components move beyond traditional data-centric security approaches toward a holistic model that tackles both data-level and network-level risks.

By unifying these elements, the framework offers a comprehensive response to persistent challenges, ranging from single points of failure in centralized systems to complex cyberattacks targeting network integrity and availability.

II. RELATED WORK

Blockchain technology has achieved significant interest across both academic and industry circles for its potential to enhance data security, improve transparency, and provide individuals with enhanced control over their own information. Early research primarily focused on understanding its foundational security models, particularly the use of cryptographic algorithms and consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS), which are critical to guaranteeing trust and maintaining data integrity within distributed systems.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

In the healthcare domain, increasing focus has been placed toward applying blockchain to address persistent challenges such as data fragmentation and concerns over patient privacy. Mandl et al. advocated for a patient-centric model where individuals retain control over access and permissions for their electronic health records (EHRs) through a system based on public standards. Building on this, Zyskind et al. proposed a system for "decentralizing privacy" by using a blockchain as an automated access-control manager that leverages pointers to manage personal data stored off-chain.This approach gave users direct the ability to own and manage their data independently of a central trusted authority. Building on this idea, Azaria et al.'s MedRec system introduced the use of smart contracts to enforce patient consent for data access while maintaining an immutable record of all interactions and modifications. This early work highlighted the potential of blockchain as a strong foundation for safeguarding data privacy and managing access.

Over time, however, the focus of research has shifted in response to more complex, network-level threats. While earlier systems largely relied on reactive security—using immutable audit trails to identify breaches after they occurred—today's systems demand a more proactive approach. This change is driven by increasingly sophisticated attacks that aim not only to compromise confidentiality but also to undermine the integrity and availability of entire networks.

Along with these concerns, scholars have recognized additional significant challenges that need to be resolved to fully realize blockchain's promise.

Hardjono et al. highlighted the issue of interoperability, noting that the rapid emergence of multiple blockchain platforms has created a fragmented ecosystem where a lack of standardized service interfaces hinders seamless cross-chain communication. Concurrently, Stoll et al. brought attention to the ecological sustainability issues linked to energy-intensive PoW consensus mechanisms, underscoring the urgent need for more energy-efficient alternatives. PoW-based Bitcoin mining, for example, is noted to generate significant carbon dioxide emissions annually, with some estimates suggesting it consumes more energy than entire countries.

The synthesis of this literature reveals a clear set of unresolved issues that form the research gap this paper addresses. Although prior research has offered a foundation for data integrity, privacy, and smart contract functionality, persistent challenges related to scalability bottlenecks, network latency, and advanced cybersecurity risks remain. The architecture proposed in this paper is presented as a direct, necessary evolution of existing solutions, moving from a primarily data-centric security model to an extensive framework that covers both data-level and network-level vulnerabilities.

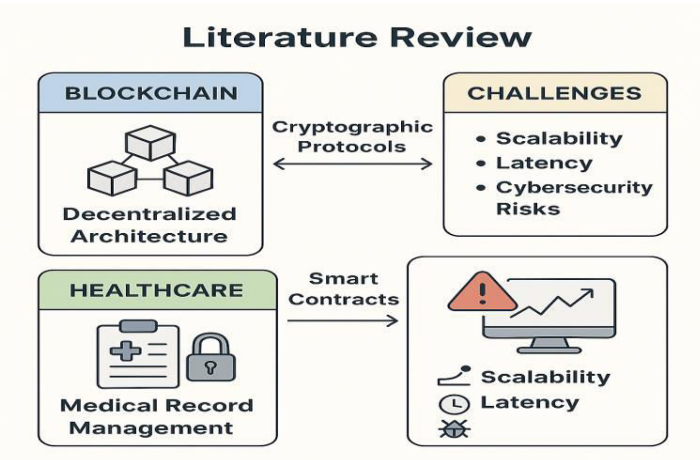

Fig 1: Related works of Literature Review

III. PROPOSED SYSTEM AND METHODOLOGY

This study introduces a security-enhanced blockchain architecture that directly addresses the vulnerabilities and limitations identified in traditional digital systems and current blockchain implementations. The framework is structured around a decentralized ledger in which every transaction is hashed and cryptographically linked to its predecessor, ensuring immutability, auditability, and tamper resistance. The system's unique capabilities are derived from the synergy of its core components, each designed to mitigate a specific set of challenges.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

A. Decentralized Node Management

The architecture distributes control throughout a distributed network of nodes, thereby eliminating dependence on a single central governing body. The distributed architecture of the framework is fundamental to ensuring resilience. By removing single points of failure, it improves fault tolerance and enhances the network's ability to withstand both large-scale disruptions and targeted attacks.With traditional centralized systems, the vulnerability of one server or authority can put the rest of the network at risk. By comparison, in the proposed design, only one node can be targeted by an attack, and the other nodes in the network can continue running safely and with high confidence under the consensus-based validation.

B. Smart Contract business layer.

A special layer within the blockchain enables one to execute smart programs as self-executing smart contracts agreed-upon agreements. This type of functionality does not involve the application of third-party interfaces and may also improve effectiveness in applications like digital identity, authorization of healthcare data, and decentralized finance. The execution of the smart contracts is deterministic and therefore the outcomes of the smart contracts should be similar and predictable throughout every node in the network. But along with those positive features, there are also a number of new weaknesses that smart contracts bring and which must be addressed. It is established that they can be applied by malicious actors to build resilient command-and-control malware infrastructures that are decentralized. Those risks are why it is essential to possess a proactive security layer that has the ability to monitoring, detecting, and addressing those threats.

C. Public Key Infrastructure (PKI) Integration

The system employs a robust Public Key Infrastructure (PKI) framework to support secure user authentication, digital signature verification, and encrypted communications. The conventional PKI is consolidated around a sole point of failure Certificate Authority(CA), the issuer, and regulator of digital instruments. Millions of individualities and deals could be at threat in a concession of CA- position. This weakness in the suggested armature is addressed by a decentralized PKI scheme, with the digital instruments and the inspection trails that are incommutable kept in the blockchain. By exploiting the decentralized and unwampered nature of the tally, the system eliminates the necessity of having a central authority. Together with current security measures and capabilities that blockchain entails, this does n't simply make it more flexible, but at least less susceptible to centralized attacks. In doing so it demonstrates a palm-palm relationship between the two technologies as the sins in one technology are exploited to balance the sins in the other technology.

D. Real- Time descry Machine

Network intrusion discovery result continually observes network business and aqueducts of deals and detects implicit security pitfalls. This element is a direct reaction to the advanced cyberattacks realized in the previous studies that include Distributed Denial-of-Service (DDoS), Sybil, and Man-in-the-Middle (MITM) attacks. Machine learning approaches such as Deep Neural Networks (DNNs) determine which network behavior is considered normal or abnormal in real time. It enables the detection and response to the threat in a timely manner by detecting abnormal trends, e.g., a sudden spike in the number of transactions (a manifestation of a DDoS attack) or the creation of multiple bogus identities (a manifestation of a Sybil attack). In addition to detection, the system may invoke intelligent controls with automated countermeasures such that the malicious action can be countered automatically without human intervention. This defense layer is proactive and operates alongside blockchain tamper-resistance functionality, which will assist in facilitating an end-to-end approach to securing digital environments.

E. Scalability and interoperability layer

To ensure that it has a long life cycle and is flexible, the architecture adopts an interoperable modular design. This strategy enables the upgrading of individual elements to fully scale with the existing blockchain platforms and legacy systems. By so doing, it directly solves the cross-chain communication barriers and fragmentation challenges identified in the preceding studies. The architecture allows broader implementation of blockchain technology into many different digital environments without undermining system integrity by allowing secure cross-chain communications and scalable deployment.

F. Improvements in Scalability and Interoperability

Though the modular architecture solves interoperability, an in-depth analysis of current scalability solutions is needed to attain the desired transaction rate. This framework includes Layer 1 and Layer 2 scaling solutions.

1) Layer 1 Scaling. Layer 1 solutions involve making changes to the core blockchain protocol. One such approach is sharding, where the network's database is split into multiple smaller, more manageable chains called "shards". This allows each shard to process transactions in parallel, rather than requiring every node to validate every transaction across the entire network. The SSchain architecture, for example, implements a two-tier system with a main root chain and a network of shards. This design helps prevent double-spend attacks by having the root chain perform additional validation on blocks created by the shards.

2) Layer 2 Scaling. Layer 2 solutions are built on top of the main blockchain to improve efficiency without altering the base layer. These solutions offload transactions from the main chain, reducing congestion and lowering fees. Examples include sidechains, which are separate blockchains running parallel to the main chain. These can be used for specific applications, with assets transferred between the main chain and the sidechain to process transactions. Other solutions like rollups and state channels also contribute to scalability by bundling multiple transactions into a single on-chain submission or by conducting thousands of off-chain transactions before recording only the final state on the main ledger.

G. Smart Contract Security

The implementation of smart contracts is foundational to the architecture's automation capabilities, but also introduces new security risks. Vulnerabilities are often rooted in coding errors, logical flaws, or insufficient access controls, with high-profile exploits resulting in millions of dollars in losses. Two common vulnerabilities addressed by this architecture's security layers are reentrancy and integer overflow/underflow attacks.

1) Reentrancy Attacks. This type of attack occurs when an external contract recursively calls a function in a vulnerable contract before the initial execution is complete. This allows the attacker to drain funds by repeatedly calling the withdrawal function before the contract's state is updated. Mitigation strategies include implementing the "checks-effects-interactions" pattern, which ensures state changes are completed before any external calls are made, and using reentrancy guards to lock a function during execution.

2) Integer Overflow/Underflow. These vulnerabilities arise when arithmetic operations exceed or fall below the limits of an integer data type. For instance, a value that exceeds the maximum limit for its type will "wrap around" to the minimum value, and a value that goes below the minimum will wrap around to the maximum. These flaws can be exploited to manipulate a contract's logic and lead to significant financial loss. Modern programming languages like Solidity version 0.8.0 and above have built-in checks to prevent this, but for older versions, libraries like SafeMath are used to perform secure arithmetic operations.

H. Cryptographic Innovations for Privacy and Efficiency

To further enhance security and privacy, this architecture integrates advanced cryptographic techniques beyond basic hashing and digital signatures.

1) Zero-Knowledge Proofs (ZKPs). ZKPs are a class of cryptographic protocols that allow one party (the prover) to prove to another (the verifier) that a statement is true without revealing any information other than the fact that it is true. This is particularly useful for protecting sensitive data, as it allows for authentication and transaction verification without exposing the underlying information. For example, a user can prove they meet certain criteria without revealing their personal data, or a company can verify compliance with a regulation without disclosing proprietary business information. ZKPs are a critical innovation for public and permissioned blockchains where some information must remain private.

2) zk-SNARKs and zk-STARKs. Two prominent types of ZKPs are zk-SNARKs and zk-STARKs. ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are known for producing compact and verifiable proofs. ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) offer enhanced security as they do not require a "trusted setup," a potential security weak point in some zk-SNARKs. They are also considered quantum-resistant, which is a key consideration for future-proofing.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

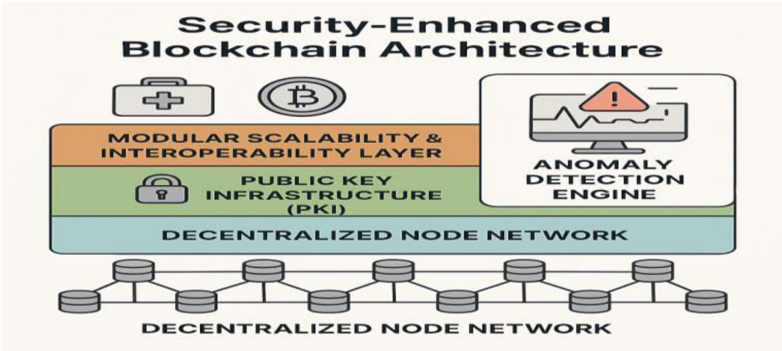

Fig 2: BlockChain Architecture Diagram

IV. IMPLEMENTATION

The proposed security-focused blockchain framework was conceptually implemented using a modular and domain-specific strategy to evaluate its functional efficiency and resilience under real-world demands. The model was deployed across two high-impact sectors: healthcare and cryptocurrency.

A. Healthcare Record Management System

In this application, patient health records are protected with asymmetric cryptography, and each user is given a dedicated public-private key pair for authentication and data exchange. Access is controlled by smart contracts that require clear and unambiguous consent from the patient and produce open and indestructible audit trails. All requests to access are logged immutably on the blockchain, maintaining data integrity and traceability across the record's lifecycle. This deployment mirrors specifically the patient data ownership and control principles suggested in previous research.

A number of practical projects, including Medicalchain and MediLedger, illustrate this model. Medicalchain enables patients to store and keep their medical records safely on the blockchain while giving them complete control and ownership. The system employs cryptographic hashing to connect records, with each hash containing a specific identifier for the contents, securing data integrity. MediLedger, a coalition of pharma firms, employs a permissioned ledger with zero-knowledge proofs for tracking and tracing prescription drugs. This enables firms to authenticate medicines and ownership while maintaining private business information confidential. The initiative proved that blockchain technology could offer one neutral platform for industry-wide data synchronization and automation.

B. Cryptocurrency Transaction Ledger (Bitcoin/Ethereum Simulation)

For digital asset management, the system employs hash chaining to preserve ledger integrity and guarantee immutability. Transactions are validated through a Proof-of-Work (PoW) consensus mechanism, enabling trustless transactions without a central authority. Smart contracts automate asset transfers, ensuring transparent, efficient, and trustless digital currency exchanges. The conceptual implementation with Bitcoin and Ethereum was chosen for its open-source frameworks, established consensus protocols, and strong support for smart contracts.

The shift from Bitcoin's energy-intensive PoW to Ethereum's more sustainable Proof-of-Stake (PoS) model is a key consideration for this architecture. PoS enhances scalability and reduces energy consumption by over 99% by having validators "stake" their currency as collateral to secure the network, rather than competing to solve complex computational puzzles. However, the transparency of PoS networks, particularly their public "mempools," can be exploited by malicious actors through methods like Maximal Extractable Value (MEV) attacks, where they front-run or reorder transactions for profit.

C. Security and Threat Mitigation Analysis

In both conceptual scenarios, the blockchain nodes are configured to continuously track system activity and transaction patterns. The Real-Time Anomaly Detection Engine analyzes these patterns to identify irregularities that may indicate cyber threats. For instance, the engine could detect a Sybil attack by identifying an unusually high number of new nodes joining the network from a limited number of IP addresses or a DDoS attack by observing an abnormal spike in transaction volume originating from a coordinated set of addresses. This dynamic security layer enhances the

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

blockchain's inherent tamper-proof structure by adding a proactive threat monitoring capability, demonstrating its potential to protect against a broader range of cybersecurity threats than current, less integrated systems.

The anomaly detection engine utilizes machine learning algorithms, such as Isolation Forest and K-means clustering, to identify irregular behaviors within the network. Isolation Forest works by isolating anomalous instances, while K-means clustering identifies abnormal instances based on their distance from normal data clusters. This allows the system to detect threats like double-spending, network congestion, or fraudulent transactions by analyzing features such as transaction size, type, or timestamp.

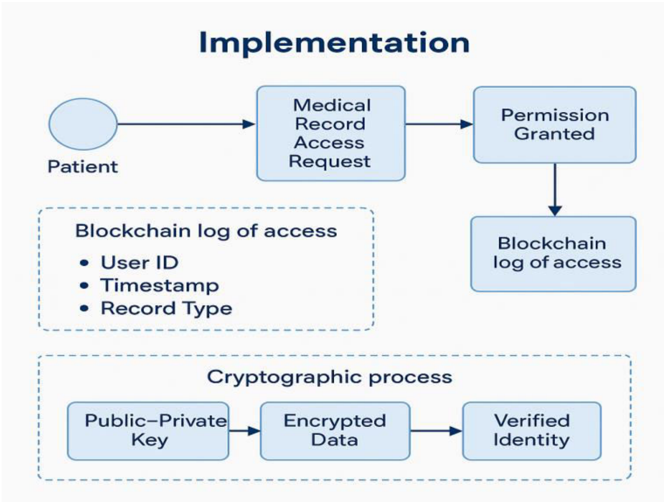

Fig 3: Implementation Diagram

V. ADVANTAGES OF THE PROPOSED SYSTEM

The proposed architecture represents a significant step forward in the development of resilient blockchain systems. The primary contributions of this work are demonstrated through the direct mitigation of the key challenges identified in the literature review, as summarized in the following table.

Table 1: Mapping of Unresolved Blockchain Security Challenges to Proposed Components and Mechanisms of Action

Unresolved Challenges	Corresponding Proposed Component	Mechanism of Action
Cybersecurity Risks (DDoS, Sybil, MITM)	Real-Time Anomaly Detection Engine	Proactively detects threats by continuously analyzing network and transactional patterns to identify and mitigate malicious behavior before it can cause disruption.
Centralized Trust Issues	Decentralized Node Management + Integration with PKI.	Removes single points of failure by keeping PKI certificates and their audit trails on an immutable distributed ledger.
Interoperability Scalability Bottlenecks.	Scalability and Interoperability Layer.	Enhances inter-chain communication and scalable deployments with integrations with other environments and legacy systems.
Smart Contracts are susceptible to.	Real-Time Anomaly Detection Engine.	Smart contracts continuously cover and make bad geste , including those who essay to use them as decentralized command and- control networks to execute malware.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

The frame illustrates a number of interrelated benefits that co-occur with others to promote stability and security. The frame is an integration of several reciprocal parcels that interact to enhance security, effectiveness and adaptability. Integrating cryptographic block linking with the decentralized agreement mechanisms are largely effective in securing the transactional data so that no bone can make an attempt to modify the data. Combined with this, the use of Public Key structure(PKI), and advanced encryption functions serve to insure the safety of data transmission, which is particularly pivotal in such a sensitive field as healthcare. Smart contracts give an fresh value of automated and rule-grounded prosecution of deals without interposers to reduce complexity, minimize costs, and enhance thickness of processes. The endless inspection trail that the frame creates through its inflexible and transparent record- keeping of information, is also vital in diligence where compliance with regulations takes priority over all other functions, including finance and logistics. Incipiently, its decentralized design, which is supported by real- time anomaly discovery systems, provides active protection against cyber attacks, guarding information integrity and vacuity.

VI. CONCLUSION AND FUTURE ENHANCEMENTS

The paper is a security- centric discussion of blockchain technology, and how it can make digital ecosystems more trusting, more private, and more automated. The proposed armature is grounded on the abecedarian capabilities of blockchain, and it combines cryptographic authentication, decentralized agreement, smart contract robotization, and it's resistant to failure and optimization. The frame demonstrates that it can be useful in practice by giving exemplifications of its operation in other diligence, similar as healthcare and cryptocurrency, where the capability to safely store sensitive information and enable unsure and automated processes is useful.

Although the proposed framework marks an important step in tackling major security risks, its success in real-world adoption will also depend on overcoming broader, non-technical hurdles. Future work should prioritize refining real-time anomaly detection, for instance by exploring the use of federated learning to balance accuracy with data privacy. Another pressing direction is the search for energy-efficient alternatives to Proof of Work (PoW), given growing concerns about the environmental impact of current approaches. In the long run, the true potential of this technology will only be realized through a combination of ongoing technical innovation, the creation of standardized interoperability protocols, and the establishment of clearer regulatory guidelines—factors that are crucial for smooth integration and global scale-up.Future research should focus on refining the proposed architecture to ensure its long-term viability and global adoption.

A. Advancing Anomaly Detection:
Future research should prioritize improving real-time anomaly detection models, with particular attention to the use of federated learning. This method enables multiple decentralized nodes to collaboratively train a shared machine learning model without exchanging raw data, thereby preserving the privacy of individual nodes and their network activity. By leveraging insights from across the network in a privacy-preserving manner, the system becomes better equipped to recognize and respond to complex, distributed attacks that might otherwise go unnoticed when observed from a single point in the system

.B. Sustainable Consensus Mechanisms:
The development of more energy-efficient alternatives to Proof-of-Work (PoW) is a critical area for continued advancement due to environmental sustainability concerns.While this paper acknowledges the transition from Proof-of-Work (PoW) to Ethereum's more sustainable Proof-of-Stake (PoS) model, further investigation is required to refine PoS and to examine alternative mechanisms such as Proof-of-Authority (PoA) and Delegated Proof-of-Stake (DPoS). The next generation of research also needs to do a comparative study of these consensus mechanisms, but not just in the sense of energy efficiency but also in the sense of the security trade-offs, their vulnerability to centralization, and their resistance to new threats, like Maximal Extractable Value (MEV) attacks.

C. Interoperability and Regulatory Frameworks:
The general adoption of blockchain technology is not only contingent on the ongoing development of new technical solutions, but also the development of standardized interoperability protocols and effective regulatory frameworks. The next round of study must be dedicated to the development of neutral, open-source standards that would allow facilitating communication on cross-chains and supporting the secure exchange of data across heterogeneous blockchain platforms. It is equally important that a transparent and supportive regulatory framework should exist that can create legal certainty and build public confidence, which is prerequisite to the global-level integration and implementation of the technology.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204070

D. **Post-Quantum Cryptography**

One of the defining problems of the future is the emergent threat of quantum computing that may disrupt the current cryptographic standards and destroy the security basis of blockchain systems. Future efforts to transform such networks into resilient and integrated long-run networks might include the addition of post-quantum cryptography (PQC) to the described architecture. It would require the design and implementation of cryptographic algorithms immune to attacks by both classical and quantum computers, and therefore offer durability against technological advancement. Examples include lattice-based cryptography, hash-based signatures, and code-based cryptography. This proactive measure is essential for future-proofing the system against a new generation of security threats.

REFERENCES

[1] http://www.blockchain4innovation.it/wpcontent/uploads/sites/4/2017/05/Blockchain-
[2] https://www.coindesk.com/information/who-created-ethereum
[3] https://www.coindesk.com/information/how-ethereum-works
[4] A Survey of blockchain security issue and challenges(Iuon-Chang Lin1,2 and Tzu-Chun Liao2)[jan-12- 2017].
[5] Public standares and patients controll:how to keep electronic medical records accessible but private(Kenneth D Mandl,Peter Szolovits,Issac S Kohane)[3 february 2001]]
[6] https://blockgeeks.com/guides/smart-contracts/
[7] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530.
[8] G. Zyskind, O. Nathan, and A. . Pentland, Decentralizing privacy:Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, May 2015
[9] https://www.researchgate.net/publication/319058582
Blockchain Challenges and Opportunities A Survey.
[10] http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf
[11] https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/securityand-privacy-in-blockchain-environments
[12] https://www.business2community.com/tech-gadgets/issues-blockchain-security- 02003488

IJARETY

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com